KU6

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America
v.

Darryl Albert Varnum

Defendant(s)

Case No. 19-2251 JMC

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of June 26, 2019 in the county of Carroll in the District of Maryland, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 115(a)(1)(A)	Threatening An Official

FILED
LOGGED
ENTERED
RECEIVED
JUL 05 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

This criminal complaint is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

Complainant's signature

Sean Wilson, Special Agent U.S. Capital Police
Printed name and title

Sworn to before me and signed in my presence.

Date: 7/5/19

Judge's signature

City and state: Baltimore, Maryland

J.Mark Coulson, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND APPLICATIONS FOR SEARCH AND SEIZURE WARRANTS

I, Sean Wilson, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of a criminal complaint against of Darryl Albert VARNUM ("VARNUM") charging him with making a threat against an official and transmitting a threat in interstate commerce in violation of 18 U.S.C. § § 115(a)910(A) and 875 (c), respectively, as well as for the issuance of warrants to search (1) the person of Darryl Albert VARNUM; (2) the personal residence of VARNUM, located at 313 Barnes Avenue, Westminster, MD 21157, to include the residence's curtilage (the "SUBJECT PREMISES"); (3) VARNUM's personal vehicle, a 2006 Red Ford F-150 Pickup Truck vehicle bearing VIN number 1FTPW14V96KC99011 and MARYLAND tag# 10X607 and registered to Darryl Albert VARNUM (the "SUBJECT VEHICLE"); and (4) an Apple iPhone 6S, IMEI 3532620796897932 (the "SUBJECT DEVICE"). The locations to be searched are described more particularly in the following paragraphs and Attachments A-1 through A-4. This affidavit is also submitted in support of a search warrant authorizing the seizure and examination of the SUBJECT DEVICE and any other electronic devices found at the SUBJECT PREMISES, and the extraction from the SUBJECT DEVICE and any other seized devices of electronically stored information. That electronically stored information, as well as the other evidence and instrumentalities to be seized, is described more particularly in the following paragraphs and in Attachment B.

2. I am a Special Agent with the United States Capitol Police (the "USCP") where I have served since January 5, 2005. I am currently assigned to the USCP Investigations Division, Threat Assessment Section ("USCP TAS"). I have completed hundreds of hours of training in

numerous areas of law enforcement investigation and techniques, including but not limited to the following: the Criminal Investigator Training Program and the Mixed Basic Police Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia; the USCP Containment Emergency Response Team Four Week Basic SWAT School; the Pentagon Force Protection Agency One Week Protective Intelligence Course; and the Metropolitan Police Department Crisis Intervention Officer Training Course. In the course of my employment as a Special Agent with the USCP, I have received training regarding the application for and execution of both search and arrest warrants. I have received training in assessing and managing individuals who have communicated threats and engaged in behaviors associated with targeted violence. In my current assignment, I have participated in and conducted numerous investigations involving illegal activity including stalking and threatening communications, both locally and interstate. As a federal law enforcement officer, I am authorized to execute search and seizure warrants under Rule 41 of the Federal Rules of Criminal Procedure.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for issuance of the Criminal Complaint and the requested warrants and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that violations of Title 18 U.S.C. § 115(a)(1)(A)(Threatening An Official) and Title 18 U.S.C. § 875(c) (Interstate Threat) have been committed by Darryl Albert VARNUM (VARNUM). There is also probable cause to believe that evidence and instrumentalities of those crimes, as more particularly described in Attachment B, will be found within the locations to be searched, which are described more particularly in Attachments A-1 through A-4.

19-2251 JMC 19-2255 JMC

PROBABLE CAUSE

5. On June 26, 2019, at approximately 7:23 PM EDT, a male person believed to be VARNUM, using phone number 443-789-9507, left a voicemail at the district office of United States Congressperson #1, which is located in the State of Florida. The voicemail, which was subsequently reported to USCP TAS on June 28, 2019, consisted of the following:

> I'm gonna kill your ass if you do that bill. I swear. I will [redacted] come down and kill your [redacted] ass. And you're a Congressperson, that is fine. I hope the [redacted] FBI, CIA, and everybody else hears this [redacted] If you're taking away my rights. This is the United States of America, [redacted] Get the [redacted] out. I will come down there and personally [redacted] kill you. I am dead [redacted] serious. I wanna see you [redacted] at my door, if you're legit. That HR bill you just pushed through, ah [redacted] you. I'll tell you what I'll come down to Miami [redacted] I'll [redacted] you up. Like Cubans don't even know.

6. An online database search of the number 443-789-9507 revealed that the current cellular carrier for that number is AT&T and that the associated user is VARNUM.

7. AT&T subscriber records, which were provided by AT&T following an emergency disclosure request made pursuant to 18 U.S.C. 2702(c)(4) for the phone number 443-789-9507, showed VARNUM to be the sole account user with a billing address of 313 Barnes Ave, Westminster, Maryland 21157 (the SUBJECT PREMISES).

8. Records provided by AT&T also identified that the telephone registered to the account is an Apple iPhone 6S, IMEI 353262079689793 2 (the SUBJECT DEVICE).

9. Location information, also provided by AT&T as a result of the emergency disclosure request, showed that on June 29 and June 30, 2019, VARNUM's cell phone was in the proximity of the SUBJECT PREMISES in Westminster, Maryland.

10. Wage records provided by the Maryland Analysis and Coordination Center ("MCAC") show that VARNUM is employed by Sealing Technologies, which is located in Columbia, Maryland.

19-2251 JMC → 19-2255 JMC

11. Vehicle records provided by MCAC show that VARNUM is the registered owner of a 2006 Ford Truck, MD Tag 10X607, VIN 1FTPW14V96KC99011.

12. Law enforcement agents in the U.S. Department of Defense Criminal Investigative Service have advised that VARNUM is currently working at the Defense Information Systems Agency ("DISA") Headquarters, located at 6914 Cooper Ave, Ft. Meade, Maryland 20755, pursuant to a contract between Sealing Technologies and DISA. DCIS further advised that because VARNUM'S job requires him to have access to sensitive information, he is prohibited from possessing a cell phone or firearms while working in the DISA building.

13. Based on my training and experience and discussions with other law enforcement officers, I know that persons who work with sensitive information in restricted areas will often use their vehicles to store items that they may not bring into the workplace, such as cell phones and firearms.

14. I have reviewed a Carroll County Sheriff's Department police report regarding an incident that occurred on May 29, 2015. According to the report, VARNUM's wife Jill English Varnum ("J. Varnum") contacted the police to report that VARNUM was having "behavioral issues." She reported that VARNUM was yelling that ISIS fighters were coming to the house to fight him and that he had taken a rifle with him into the garage. J. Varnum told the police that VARNUM seemed to be intoxicated and that he owned "numerous guns." The report further indicated that when police arrived, VARNUM told them that Taliban fighters were coming to his house and that he had been drinking vodka. According to the report, VARNUM was cooperative and non-violent in his interaction with the police and he was transported to a hospital for a mental health evaluation.

15. Records provided by the Maryland State Police Firearms Licensing Office show that VARNUM has registered to him a Ruger .45 caliber pistol, model KP345PR, serial #66420301. VARNUM does not have a concealed carry permit or any other firearms licenses.

16. I have located a public Facebook account in the name of "Darryl Varnum" with a spouse identified as "Jill Varnum." On June 26, 2019 at 7:35PM EDT, approximately 12 minutes after the threatening voicemail was left at Congressperson #1's office, a post appeared on the public timeline of that Facebook account which included a photograph of an American flag and the words "H.R. 2527 Vaccinate All Children Act of 2019." The post also stated the following: "Holocaust has begun! I'm done with this bullshit. Time to step up or ship out!" At 8:10 pm that same day, a post appeared on the timeline stating: "All of our guns are next, been trying for years!"

17. Open source research identifies Congressperson #1 as a public supporter of H.R. 2527.

18. Based on my training and experience and discussions with other law enforcement officers, I know that persons committing or intending to commit threat-related offenses often utilize computers, data storage devices (e.g., external storage devices, ZIP disks, and CD-Roms), and other electronic communications equipment, including cellular telephones, to search the internet, to store plans and conduct research related to attacks or threat-related activities, and to communicate and transmit threats to recipients of threat-related activities.

UNLOCKING ELECTRONIC DEVICES USING BIOMETRIC FEATURES

19. I know from my training and experience, as well as publicly available materials, that encryption systems for mobile phones and other electronic devices are becoming ever more widespread. Such encryption systems protect the contents of these devices from unauthorized

access by users, and render these contents unreadable to anyone who does not have the device's password. As device encryption becomes more commonplace, the encryption systems implemented by device manufacturers are becoming more robust, with few—if any—workarounds available to law enforcement investigators.

20. I also know that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

21. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. Examples of devices providing a fingerprint unlocking capability are several models of Apple's iPhone. Apple iPhones may be fingerprint unlocked using a function called Touch ID, which during setup allows for registering as many as five (5) fingerprints to unlock the device. The number of electronic devices providing a fingerprint unlocking capability, including both smart phones and laptops, is growing continually.

22. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other

manufacturers have different names but operate similarly to Windows Hello.

23. In my training and experience, users of electronic devices often enable the above-mentioned biometric features because they are considered a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. In some instances, biometric features are considered a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

24. Related to the above discussion regarding encryption, if a forensic examination is not conducted shortly after seizing the device while it is in an unlocked state, or unlocking the device using biometric features immediately upon seizing it, law enforcement investigators may completely lose the ability to forensically examine the device, assuming the device's owner refuses to disclose the password. The passcode or password that would unlock any such device subject to search under these warrants is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device, making the use of biometric features necessary to the execution of the search authorized by these warrants.

25. Biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: 1) more than 48 hours has elapsed since the device was last unlocked; or 2) when the device has not been unlocked using a fingerprint for eight (8) hours *and* the passcode or password has not been entered in the last six (6) days. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

26. Due to the foregoing, if law enforcement personnel encounter a device that is subject to seizure pursuant to these warrants and may be unlocked using one of these biometric features, the warrants I am applying for would permit law enforcement personnel to: 1) press or swipe the fingers (including thumbs) of any individual, who is reasonably believed by law enforcement to be a user of the device(s), to the fingerprint scanner of the device(s); and/or 2) hold the device(s) in front of the face of those same individuals and activate the iris recognition feature, for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by these warrants. In the event that law enforcement is unable to unlock the subject device(s) within the number of attempts permitted by the pertinent operating system, this will simply result in the device(s) requiring the entry of a password or passcode before it can be unlocked.

27. Due to the foregoing, I request that the Court authorize law enforcement personnel to press the fingers (including thumbs) of VARNUM or any other individual who is in possession of the SUBJECT DEVICE, and any other individuals who may be present during the search of the SUBJECT PREMISES, to unlock the SUBJECT DEVICE and any other electronic devices that may be seized at the SUBJECT PREMISES so that investigators may conduct the search and examination as described in this Affidavit and Attachment B.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

28. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, the SUBJECT VEHICLE and VARNUM's person, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. Thus, the

warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. *Probable cause.* I submit that if a computer or storage medium is found on or in the SUBJECT PREMISES or SUBJECT VEHICLE, or on VARNUM's person, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES or SUBJECT VEHICLE or on VARNUM's person, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

19-2255 JMC

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

31. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily

viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

32. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

19-2251 JMC

19-2255 JMC

AUTHORIZATION REQUEST

33. Based on the foregoing, I respectfully submit that there is probable cause to believe that VARNUM threatened to kill Congressperson #1 in violation of 18 U.S.C. § 115 (a)(1)(A) and that VARNUM transmitted his threat via telephone from his location in Maryland to the office in Florida in violation of 18 U.S.C. § 875(c). I request that a criminal complaint, arrest warrant and search and seizure warrants be issued, as prayed.

REQUEST FOR SEALING

34. I further request that the Court order that the affidavit in support of the criminal complaint and search warrants be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to the target of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation, including by giving the individual under investigation an opportunity to destroy or tamper with evidence, change patterns of behavior, notify confederates, and flee from prosecution.

Respectfully submitted,

Sean Wilson
Special Agent
U.S. Capitol Police

FILED ENTERED
LOGGED RECEIVED
JUL 05 2019
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY DEPUTY

Subscribed and sworn to before me on July 5, 2019.

The Honorable J. Mark Coulson
United States Magistrate Judge